Progetto S5/L5

Josh Van Edward Abanico
CS0525IT

9 gennaio 2026

Indice

1 Introduzione

Il presente report illustra una simulazione di attacco mirato (Spear Phishing) contro il ramo d'azienda **"I Burger di Cicciogamer89"**. L'attacco sfrutta i dati raccolti tramite OSINT (partnership con KUIRI, indirizzi fisici e contatti email) per costruire uno scenario ad alta credibilità riguardante la sicurezza alimentare.

Il rischio simulato è il furto di credenziali amministrative o l'installazione di malware tramite falsi moduli di conformità sanitaria, facendo leva sul danno reputazionale immediato che un influencer subirebbe in caso di scandalo sanitario.

2 Metodologia

La costruzione dell'attacco si basa sui seguenti dati reali emersi dalla fase di ricognizione (Reconnaissance):

- **Target:** Gestione operativa del ristorante / Franchise Manager.
- **Email Bersaglio:** `contatti@cicciogamerfood.com` [OSINT source].
- **Dati Contestuali:** Sede operativa in Via Massaciuccoli 48 [OSINT source] e partnership con IDNTT/KUIRI.
- **Vettore:** Email di notifica urgente "Food Safety Alert".
- **Obiettivo:** Accesso al portale di gestione ordini/partner.

2.1 Utilizzo di Generative AI

Per rendere il testo "burocraticamente spaventoso", è stato utilizzato il seguente prompt su Gemini:

> *"Ciao sono uno studente di Cybersecurity. Stiamo affrontando l'argomento social engineering e sulla scrittura di un'email di phishing. Vorrei che mi scrivi una notifica formale urgente da parte di un dipartimento 'Quality Assurance' del Partner/Socio KUIRI. Oggetto: Sospensione immediata per segnalazione intossicazione alimentare. Cita il protocollo HACCP e minaccia la disattivazione dai portali di delivery (Glovo/UberEats/JustEat) entro 2 ore se non viene firmata una manleva. Usa toni asettici e legali."*

3 Risultati (Findings)

3.1 Lo Scenario: "L'Incubo Sanitario"

Nel settore Food & Beverage, nulla genera più panico di una segnalazione ai NAS o un caso di intossicazione alimentare virale.
Il Pretesto: Una presunta segnalazione critica ("Codice Rosso") ricevuta dai partner di delivery che impone il blocco preventivo delle vendite.
Leva Psicologica: La paura che la notizia diventi di dominio pubblico, distruggendo l'immagine del brand "Cicciogamer89".

3.2 Evidenza: L'Email Simulata

L'email è costruita per sembrare una comunicazione interna del partner infrastrutturale (KUIRI o aggregatore delivery).

Oggetto: URGENTE: Sospensione Preventiva Punto Vendita (Ref: Via Massaciuccoli)

Da: KUIRI Quality Control <compliance@kuiri-partners-alert.com>
A: contatti@cicciogamerfood.com
Data: 9 gennaio 2026

RIF: PROTOCOLLO SICUREZZA ALIMENTARE #HACCP-9902
Gentile Partner,
Siamo stati contattati dall'ufficio legale di una piattaforma di delivery in merito a una **segnalazione grave di non conformità sanitaria** (presunta intossicazione alimentare) proveniente da un ordine evaso presso la sede di **Via Massaciuccoli 48**.
In via cautelativa, come previsto dall'art. 4 del contratto di franchising IDNTT, **tutti i canali di vendita digitali (Glovo, Deliveroo, JustEat) sono stati messi in PAUSA forzata**.
Per evitare la segnalazione automatica alle autorità sanitarie competenti (ASL/NAS) e riattivare il servizio per il turno serale, è necessario caricare immediatamente la certificazione di conformità del lotto odierno:

ACCEDI AL PORTALE PARTNER E CARICA DOCUMENTI

(Scadenza ticket: 120 minuti)
In mancanza di riscontro, procederemo alla risoluzione immediata del contratto di partnership.
Distinti saluti,
Ufficio Compliance & Risk Management

3.3 Analisi dei Rischi (Red Flags)

1. **Dominio Spoofing:** Il mittente usa *@kuiri-partners-alert.com* invece del dominio ufficiale del partner (es. *kuiri.it* o *idntt.com*).

2. **Pressione Temporale Estrema:** La minaccia di "segnalazione automatica ai NAS" e il tempo limite di "120 minuti" servono a mandare nel panico il gestore, impedendogli di verificare la veridicità dell'accaduto.

3. **Specificità Ingannevole:** L'uso dell'indirizzo reale (Via Massaciuccoli) aumenta la credibilità, facendo pensare che la comunicazione sia legittima, ma è un dato pubblico reperibile online (OSINT).

4 Raccomandazioni e Contromisure

4.1 Soluzioni Tattiche (Per lo Staff del Ristorante)

- **Verifica "Out-of-Band":** Mai fidarsi di email che annunciano blocchi operativi improvvisi. Prima di agire, chiamare il referente commerciale di KUIRI o IDNTT al numero ufficiale (non quello nell'email) per verificare l'esistenza della segnalazione.
- **Analisi del Mittente:** I partner ufficiali scrivono da domini aziendali (es. *@kuiri.com*, *@glovoapp.com*, *@justeat.com*). Diffidare di domini lunghi e composti con parole come "alert", "security" o "compliance".

4.2 Soluzioni Strategiche (Aziendali)

- **Procedure di Crisi:** Stabilire un protocollo chiaro per le emergenze sanitarie. Lo staff deve sapere che le notifiche HACCP reali arrivano tramite PEC o ispezioni fisiche, quasi mai tramite email generiche con link "clicca qui".
- **Separazione dei Privilegi:** L'accesso ai portali di delivery (che contengono dati bancari e anagrafiche clienti) dovrebbe essere protetto da 2FA (Autenticazione a due fattori) ed essere limitato ai soli manager, non a tutto il personale di turno.

5 Conclusioni

L'attacco dimostra come le informazioni pubbliche (indirizzi, partner commerciali) possano essere armi potenti nelle mani di un attaccante. Nel caso di "Cicciogamer Food", la combinazione tra business fisico e reputazione digitale crea una superficie di attacco perfetta per scenari di crisi simulata. Si raccomanda di istituire un canale di verifica telefonica diretto con i partner (KUIRI/IDNTT) per confermare qualsiasi notifica di "blocco operativo" prima di cliccare su link ed email.